JOSHUA D. BRANSON*
jbranson@kellogghansen.com
DANIEL V. DORRIS*
ddorris@kellogghansen.com
BETHAN R. JONES**
bjones@kellogghansen.com
MATTHEW D. READE*
mreade@kellogghansen.com
TIBERIUS T. DAVIS*
tdavis@kellogghansen.com
KELLOGG, HANSEN, TODD,
FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
Telephone: (202) 326-7900
Facsimile: (202) 326-7999
* *Admitted Pro Hac Vice*

ADRIAN SAWYER, State Bar No. 203712
sawyer@sawyerlabar.com
SAWYER & LABAR LLP
1700 Montgomery Street, Suite 108
San Francisco, California 94111
Telephone: (415) 262-3820

Counsel for Plaintiff
X Corp.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

X CORP., a Nevada corporation,

Plaintiff,

v.

BRIGHT DATA LTD., an Israeli corporation,

Defendant.

Case No. 3:23-cv-03698-WHA

PLAINTIFF'S NOTICE OF MOTION AND MOTION FOR LEAVE TO FILE A SECOND AMENDED COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT

Judge: Hon. William H. Alsup
Date: September 26, 2024
Time: 8:00 a.m.
Crtrm: 12, 19th Floor

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

RULE

REGULATIONS

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE THAT the hearing on X Corp.'s ("X") Motion for Leave To File a Second Amended Complaint will take place on September 26, 2024 at 8:00 a.m. or as soon thereafter as the matter may be heard before the Honorable William H. Alsup, United States District Court Judge for the Northern District of California, Courtroom 12, 19th Floor, 450 Golden Gate Avenue, San Francisco, CA 94102.

Plaintiff X moves this Court, pursuant to Rule 15(a)(2) of the Federal Rules of Civil Procedure, for leave to file a Second Amended Complaint. This Motion is based on this Notice of Motion and Motion, the Memorandum of Points and Authorities set forth below, the Exhibits to this Motion, the accompanying Declaration of Joshua D. Branson, the other documents on file in this action, and any oral argument of counsel at the hearing on the Motion.

STATEMENT OF ISSUES TO BE DECIDED

1. Whether the Court should grant X's Motion for Leave To File its Amended Complaint.
2. Whether the Second Amended Complaint adequately alleges an injury for X's access-based claims of trespass to chattels, tortious interference with contract, and breach of contract.
3. Whether the Second Amended Complaint adequately alleges violations of California Business and Professions Code § 17200.
4. Whether the Copyright Act impliedly preempts the scraping-based claims alleged in the Second Amended Complaint.
5. Whether the Second Amended Complaint states additional claims for violations of the Digital Millennium Copyright Act, the Computer Fraud and Abuse Act, and California's Comprehensive Computer Data and Access Fraud Act.

I. INTRODUCTION

Plaintiff X Corp. ("X") moves for leave to file the attached Second Amended Complaint ("SAC") against Defendant Bright Data Ltd. ("Bright Data"). The SAC supplements X's allegations to remedy the pleading issues the Court's earlier opinion identified. The SAC also adds three new claims under the federal Digital Millennium Copyright Act, the federal Computer Fraud and Abuse Act, and California's Comprehensive Computer Data and Access Fraud Act.

The SAC resolves the concerns that led the Court to dismiss X's last complaint. Following the Court's invitation, the SAC now alleges significant, quantifiable harms inflicted by Bright Data's serial intrusions into X's servers, including diminished server capacity and a degraded user experience. Those new allegations supply the concrete facts the Court said were missing from X's earlier access-based claims. The SAC also supplements X's scraping claims to show that the Copyright Act does not preempt them. Indeed, the new allegations clarify that X's claims do not conflict with the federal copyright regime, but rather promote independent state interests in user privacy and data security. And the three new claims – including two under federal law – avoid the Court's preemption concerns altogether. The new claims arise from the same factual allegations and are themselves enough to survive a motion to dismiss. Amending to add them is not futile. And none of Rule 15(a)(2)'s other factors warrant denying leave to amend at this early stage. The Court should grant the motion and accept the SAC.

II. BACKGROUND

X sued Bright Data in July 2023 for breach of contract, tortious interference with contract, and unjust enrichment stemming from Bright Data's unlawful access to X's platform, scraping and selling of X's data, and facilitating others to do the same. Dkt. 1. X amended its complaint in November 2023 as a matter of course to add claims for trespass to chattels, violation of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200 *et seq.*, and misappropriation. Dkt. 36. The Court declined to dismiss the complaint on personal-jurisdiction grounds, Dkt. 67, but later dismissed X's claims for two core reasons, Dkt. 83 ("Op."). First, the Court dismissed X's access-related claims for failing to adequately allege that Bright Data's access to X's systems caused X any concrete harm. *Id.* Second, the Court

found that the Copyright Act impliedly preempts X's scraping claims, which the Court viewed as failing to allege any independent state interest apart from copyright. *Id.*

The Court invited X to "seek leave to amend" to cure those concerns. *Id.* at 26. X's prior counsel timely sought leave, but the Court disqualified counsel and instructed "[s]hould X Corp. wish to move for leave to amend its complaint, a new motion prepared by someone else is due [by August 16]." Dkt. 105 at 15. X's new counsel now files this motion. It attaches the proposed SAC, a redlined copy showing changes, and a proposed order. Exhs. A-C.

III. LEGAL STANDARD

Courts must "freely give leave" to amend pleadings "when justice so requires." Fed. R. Civ. P. 15(a)(2). That rule contemplates "extreme liberality." *Eminence Cap., LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1051 (9th Cir. 2003) (cleaned up). Courts consider: "(1) bad faith; (2) undue delay; (3) prejudice to the opposing party; (4) futility of amendment; and (5) repeated failure to cure deficiencies." *Shelton v. Comercia Bank*, 2024 WL 234721, at *2 (N.D. Cal. Jan. 22, 2024) (Alsup, J.). Prejudice "carries the greatest weight," *id.* at *1 (quoting *Eminence*, 316 F.3d at 1052), and "the party opposing amendment bears the burden of showing prejudice," *DCD Programs, Ltd. v. Leighton*, 833 F.2d 183, 187 (9th Cir. 1987).

To deny leave for futility, "the Court must be satisfied that 'no set of facts can be proved under the amendment to the pleadings that would constitute a valid and sufficient claim.'" *Robertson v. Bruckert*, 568 F. Supp. 3d 1044, 1048 (N.D. Cal. 2021) (quoting *Miller v. Rykoff-Sexton, Inc.*, 845 F.2d 209, 214 (9th Cir. 1988)). "[T]he legal standard is the same as it would be on a motion to dismiss under FRCP 12(b)(6)." *Bronson v. Samsung Elecs. Am., Inc.*, 2019 WL 174526, at *1 (N.D. Cal. Jan. 10, 2019) (Alsup, J.) (finding amendment not futile). The Court should thus continue to "accept as true all well-pleaded allegations of material fact, and construe them in the light most favorable to the non-moving party." *Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998 (9th Cir. 2010). This Court "liberally grant[s]" amendment where, "from the underlying facts or circumstances, the plaintiff may be able to state a claim." *Sonos Inc. v. Google LLC*, 2022 WL 2046828, at *2 (N.D. Cal. June 7, 2022) (Alsup, J).

IV. ARGUMENT

The SAC cures the concerns that prompted the Court to dismiss X's prior claims. *First*, the SAC plausibly alleges "damage . . . resulting from [Bright Data's] access through unauthorized means," Op. at 15-17, as well as new facts and statutory violations reviving its UCL claim, *id.* at 11-13. *Second*, the SAC explains that X's scraping-based claims vindicate non-copyright interests sufficient to shield them from conflict preemption. *Id.* at 25. *Third*, the SAC alleges three new claims that avoid the Court's concerns altogether. These amendments are not futile, and there is no other basis for denying X leave to file them under Rule 15.

A. X's Amendments To Its Existing Claims Are Not Futile

1. The SAC Plausibly Alleges Access-Based Claims

The Court dismissed X's access-based claims for lacking adequate allegations of injury. Op. at 9-11, 14-17. The SAC addresses that concern by alleging that Bright Data's (and its customers') intrusions into X's systems diminishes X's server capacity, degrades its user experience, and requires it to spend money managing the resulting strain on its infrastructure.

Bright Data harms X by barraging its servers with massive numbers of automated data requests. SAC ¶¶ 80-95. X receives [redacted] of requests each day that are "inauthentic" and attributable to automated bots or software. *Id.* ¶ 87. Those inauthentic requests [redacted] and degrade the experience for legitimate users of the platform. *Id.* ¶¶ 89, 95. The harm is especially pronounced for several of X's key end points that suffer from unusually high volumes of inauthentic requests. For example, inauthentic or anomalous requests account for [redacted] of attempts to view [redacted] of requests to access [redacted] of requests to view [redacted] of requests to find [redacted] *Id.* ¶ 87. To mitigate the server strains caused by the deluge of unauthorized requests targeting these end points, X must [redacted]. *Id.* ¶¶ 89-90. Otherwise, inauthentic web requests would cause X's servers to fail more regularly, worsening the user experience. *Id.* ¶ 91.

Data scraping contributes substantially to that avalanche of inauthentic data requests. *Id.* ¶¶ 82-84. Data scraping necessarily involves sending "large volumes – in the millions or even billions – of these requests, taxing the capacity of servers and diminishing the experience for legitimate users." *Id.* ¶ 59. Ordinary human users cannot similarly bombard X's endpoints with [redacted] of sequential data requests. *Id.* ¶ 83. Unsurprisingly, then, [redacted]." *Id.* ¶ 83. For example, at various times [redacted] of all requests for [redacted] were coming from data scrapers; data scrapers were submitting [redacted]; and [redacted] traffic originated from data scrapers. *Id.* ¶ 88. Scrapers also target the very endpoints noted above – which scrapers value more than ordinary human users do – that suffer disproportionate volumes of inauthentic requests. *Id.* ¶¶ 87-89. And the problem is only worsening: Bright Data itself describes scraping as growing 46.5% a year. *Id.* ¶ 85.

Bright Data bears the blame for this profusion of harmful data scraping. It has cultivated a reputation as the "market leader" in scraping data from social-media platforms like X. *Id.* ¶ 111. Not only does Bright Data engage in scraping itself; it also sells tools enabling others to do so. *Id.* ¶¶ 105-31. In fact, Bright Data is the industry's largest purveyor of proxy servers that generate an endless supply of rotating, fake IP addresses designed to evade X's technological safeguards. *Id.* ¶¶ 108-11, 129-32. Bright Data flaunts its Web Scraper, for example, as allowing scrapers to "[g]ather vast amounts of public web data with total anonymity." *Id.* ¶¶ 123, 131. That "total anonymity" impedes X from pinpointing every instance where Bright Data or its customers have accessed X's systems. *Id.* ¶¶ 112-13, 131. Such calculated anonymity further strengthens the inference of harm. Because Bright Data purposefully seeks to evade detection, discovery is warranted to confirm the degree to which it is responsible for the deluge of inauthentic web requests straining X's infrastructure. *See Soo Park v. Thompson*, 851 F.3d 910, 928 (9th Cir. 2017) (dismissal inappropriate "where the facts are peculiarly within the possession and control of the defendant") (cleaned up); Op. at 14 (recognizing "X Corp. would not have had access to Bright Data customer information when drafting" complaint).

These new allegations remedy the Court's concern that X did not adequately allege "damage resulting from access through unauthorized means." Op. at 17. Having rectified that concern, the SAC now states a claim for trespass to chattels, tortious interference with contract, and breach of contract based on Bright Data's unauthorized access of X's platform. *See id.* at 8-18 (addressing these claims). For the same reasons, X sufficiently pleads injury under the UCL. The SAC further adds allegations addressing the other deficiencies the Court found with that claim. *See id.* at 11-12. We briefly address the elements of each claim below.

a) Trespass to Chattels

Trespass to chattels requires that an "intentional interference with the possession of personal property has proximately caused injury." Op. at 9 (quoting *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1350-51 (2003)). Bright Data's scraping activities meet that test by straining X's servers, [redacted], and degrading the user experience. *Supra* pp. 4-5.

The new allegations mirror those in *hiQ Labs, Inc. v. LinkedIn Corp.*, 2021 WL 1531172 (N.D. Cal. Apr. 19, 2021), which this Court previously highlighted. Op. at 10 (citing *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1113 n.11 (N.D. Cal. 2017) ("Such attacks are likely remediable under, *e.g.*, the common law tort of trespass to chattel."), *aff'd*, 31 F.4th 1180 (9th Cir. 2022)). LinkedIn there alleged that it received millions of unauthorized requests a day, that scrapers in the aggregate "place a substantial burden on LinkedIn's infrastructure," and that the "full extent of hiQ's illicit scraping is not currently known." *hiQ*, 2021 WL 1531172, at *10 (cleaned up). Judge Chen upheld those injury allegations, reasoning that "requests generated by hiQ's bots burden LinkedIn's servers" and so inflict injury sufficient "to support a request for injunctive relief." *Id.* X likewise alleges that Bright Data's scraping entails a barrage of inauthentic requests that "burden [X]'s servers." *Id.*; *see* SAC ¶¶ 68-72, 86-95, 120-31. As in *hiQ*, that states a trespass-to-chattels claim. *See also eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000) (80,000 to 100,000 requests plausibly caused injury by consuming "at least a portion of plaintiff's bandwidth and server capacity").

The SAC also answers the Court's question whether automated scraping requests are "inherently burdensome" for X to absorb. Op. at 9. As now alleged (SAC ¶¶ 83-89), scraping-

driven requests are far "more burdensome than an X user sending requests to X Corp.'s servers with a browser." Op. at 9. That is due mainly to their scale. Unlike legitimate users, Bright Data and its customers circumvent X's rate limits to query X's servers repeatedly, at volumes that far outstrip anything ordinary human users do. SAC ¶¶ 59, 71-72, 82-83. And Bright Data employs (and sells) tools that mask scrapers' IP addresses to prevent X from modulating or slowing their repeated requests. *Id.* ¶ 132. For that reason, X's [redacted]. *Id.* ¶ 83. And unlike ordinary users, scrapers make mass requests that sweep in less-popular posts that X has not cached, which are far less efficient for X to serve than the type of posts on which regular users focus. *Id.* The resulting burden on X's systems is significant and unique. *Id.* ¶¶ 83-95. These allegations show the "actual or threatened interference with [X's] computers' functioning" that California law requires. *Intel*, 30 Cal. 4th at 1353.

The SAC similarly refutes Bright Data's earlier argument that it cannot be liable for trespass to chattels because X "consented to participate" in scraping "when it connected its servers to the Internet." Dkt. 42 at 23. In a nearly identical case, Judge Whyte rejected the same argument that data was "publicly accessible," observing that "[e]ven if [defendant]'s web crawlers were authorized to make individual queries of [plaintiff's] system, [defendant's] web crawlers exceeded the scope of any such consent when they began acting like robots by making repeated queries." *eBay*, 100 F. Supp. 2d at 1070. Here, too, both X's Terms and its robots.txt file – which tells bots like Bright Data's which content they are permitted to access – make clear that X never consented to automated, mass usage. SAC ¶¶ 29-35, 75-89.

California's trespass-to-chattels doctrine has long recognized that property owners may consent to *limited* access while imposing liability on those who "proceed[] to exceed those limits by divergent conduct." *Civic W. Corp. v. Zila Indus., Inc.*, 66 Cal. App. 3d 1, 17 (1977). Bright Data has far exceeded X's consent, placing its conduct "outside the range of the ordinary activity involved" in accessing X's platform. *Knight v. Jewett*, 3 Cal. 4th 296, 318 (1992). That is enough to state a trespass-to-chattels claim.

b) Tortious Interference with Contract

As the Court has held, X sufficiently alleges that Bright Data induced its customers to breach valid, enforceable contracts with X. Op. at 14-15. But the Court ruled that X's last complaint "ha[d] not alleged any damage resulting from automated access to systems." *Id.* The new allegations plug that gap. Bright Data markets web-scraping tools to its customers to enable them to anonymously scrape data from X. SAC ¶ 131. Those tools spawn a massive number of inauthentic requests, especially for servers hosting data that scrapers most desire. *Id.* ¶¶ 83-92. Those requests cause X the same types of injuries outlined above. *Supra* pp. 4-5. The new allegations also establish that, but for Bright Data's tools, Bright Data's customers would have needed to join X's API program to obtain the data they want. SAC ¶¶ 39-51, 58-59. X's lost revenue from those stolen business opportunities constitutes cognizable injury.

c) Breach of Contract

The Court similarly ruled that Bright Data is "bound by the Terms [restricting accessing or scraping X's platform], having impliedly agreed to them in ongoing scraping." Op. at 15-17. As with the tortious-interference claim, however, the Court previously discerned a lack of allegations showing "damage resulting from access through unauthorized means." *Id.* at 17. The SAC adds those allegations. Further, the SAC now alleges expectation damages from Bright Data's breach. Bright Data exploited free user accounts to avoid paying for X's API, depriving X of the revenue it would have earned. SAC ¶¶ 47, 58-59.

d) UCL

The UCL provides a cause of action for any unfair, fraudulent, or unlawful business practice. Cal. Bus. & Prof. Code § 17200. "Each of these 'prongs' under the UCL creates an independent theory of liability." *Eidmann v. Walgreen Co.*, 522 F. Supp. 3d 634, 643 (N.D. Cal. 2021). The Court dismissed X's prior UCL claim because the last complaint failed to allege an "unfair business act" or, for purposes of the UCL's "fraudulent" prong, a misrepresentation. *See* Op. at 11-12. The Court also found that the amended complaint "fail[ed] to state a predicate claim" showing an unlawful business act. *Id.* at 11. The SAC remedies those deficiencies.

First, an unfair act includes a business "practice that offends established public policy, or is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *Pirozzi v. Apple, Inc.*, 966 F. Supp. 2d 909, 921 (N.D. Cal. 2013). The SAC alleges that Bright Data's business practices allow Bright Data and others to circumvent technological restrictions designed to protect users' privacy rights, *see* SAC ¶¶ 58-79; *infra* pp. 15-17, which violates "California's public policy of protecting customer data," *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 990 (N.D. Cal. 2016) (members of health care plans whose personal information was exposed to hackers adequately alleged that company's failure to prevent cyber-attack violated UCL's unfair prong); *In re Adobe Sys., Inc. Priv. Litig.*, 66 F. Supp. 3d 1197, 1227 (N.D. Cal. 2014) (similar allegations sufficient for software subscribers whose personal information was compromised in a data breach to state a claim under UCL's unfair prong).

Second, in finding that X failed to allege a fraudulent business act, the Court concluded that X had alleged scraping of only *public* data, making Bright Data and its customers "legitimate X users who were under no obligation to log in." Op. at 12. But the SAC clarifies that much of the data Bright Data and its customers scrapes is *not* available to the public. *See* SAC ¶¶ 25-28, 64-70; *infra* pp. 14-15. Indeed, the SAC alleges that Bright Data's tools allow its customers to gain access to password-protected data using proxy servers and fake accounts, even for scrapers that X had already blocked. SAC ¶ 132. That is just what the Court posited could allege a misrepresentation under the UCL's "fraudulent" prong. *See* Op. at 13.

Third, because the SAC both cures the concerns that prompted the Court to dismiss X's previous claims and pleads new statutory violations, *infra* pp. 19-23, the SAC plausibly alleges "unlawful conduct that may serve as a basis for a claim under the UCL's unlawful prong." *In re Adobe Sys.*, 66 F. Supp. 3d at 1226. The Court should thus accept the amended UCL claim.

2. The Amended Scraping Claims Are Not Impliedly Preempted

The SAC also pleads scraping-based claims that the Copyright Act does not preempt. In its prior order, the Court held correctly that the Copyright Act's express-preemption clause does not apply because X asserts state-law rights that "are not 'equivalent' to rights created by

copyright law." Op. at 22; *see* 17 U.S.C. § 301(a). But it discerned implied conflict preemption because it viewed X's claims as "*undermin[ing]* federal copyright law." Op. at 21-22.

X respectfully disagrees with the Court's preemption ruling. The Supreme Court disfavors implied-conflict preemption, which "elevate[s] abstract and unenacted legislative desires above state law" at a "cost[] to cooperative federalism and individual liberty." *Virginia Uranium, Inc. v. Warren*, 587 U.S. 761, 775-79 (2019). For that reason, a "high threshold must be met before a court" will find implied obstacle preemption unmoored from a statute's text. *In re Volkswagen "Clean Diesel" Mktg., Sales Pracs., & Prods. Liab. Litig.*, 959 F.3d 1201, 1212 (9th Cir. 2020) (cleaned up). Bright Data cannot meet that threshold here, where the Copyright Act already includes an express-preemption clause delineating the statute's preemptive force. 17 U.S.C. § 301(a). Indeed, Congress disclaimed any intent to preempt state law for "activities violating legal or equitable rights that are not equivalent to any of the exclusive rights within the general scope of copyright." *Id.* § 301(b)(3); *see Alberghetti v. Corbis Corp.*, 2009 WL 10673207, at *4 (C.D. Cal. Oct. 27, 2009) (applying § 301(b)(3) to mean "this Court is not empowered to use conflict preemption" to dismiss state-law claims outside preemption clause).

That said, the SAC's amended claims survive preemption under the Court's prior analysis. Copyright conflict preemption turns on (i) whether X's state-law claims conflict with the Copyright Act's "purpose"; and (ii) whether those claims "vindicate[] a substantial state law interest" distinct from copyright. Op. at 23-25. Both factors disfavor preemption here.

a) X's amended claims do not undermine the federal copyright regime

Conflict preemption extinguishes state laws that "stand[] as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Ryan v. Editions Ltd. W.*, 786 F.3d 754, 761 (9th Cir. 2015) (cleaned up). The Copyright Act's purpose is "[t]o promote the Progress of Science and useful Arts" by "assur[ing] authors the right to their original expression" while also "encourag[ing] others to build freely upon the ideas and information conveyed by a work." *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 349-50 (1991) (cleaned up). The SAC's claims alleging Bright Data's mass automated scraping of data from X's platform do not undermine that purpose.

Contract claims. X's breach-of-contract and tortious-interference claims do not conflict with the Copyright Act. Federal copyright law sets default rules governing a "copyright holder's efforts to enforce its rights against the world." *Ryan*, 786 F.3d at 762. The SAC's contract claims, by contrast, involve "one party to a contract enforcing [its] rights against [its] contracting partner." *Id*. As the Ninth Circuit explained, "enforcement" of such "private agreement[s] . . . poses no serious obstacle" to federal copyright policy. *Id*. (fee-shifting contract that departed from Copyright Act fees provision). That is why "[m]ost courts have held that the Copyright Act does not preempt the enforcement of contractual rights." *Altera Corp. v. Clear Logic, Inc.*, 424 F.3d 1079, 1089 (9th Cir. 2005) (collecting cases).[1] Put simply, the statute allows private "parties to contract away" copyright law's default rules. *Davidson*, 422 F.3d at 639.

Those principles are decisive here. The SAC alleges that Bright Data intentionally breached – and induced others to breach – contract terms that Bright Data knowingly accepted by registering accounts and using X's platform. SAC ¶¶ 23-35, 96-104, 114-31. As the Court recognized, these allegations support a plausible inference that Bright Data had "actual knowledge of the Terms at all relevant times" and so bound itself to "an existing enforceable contract." Op. at 16; *see id*. at 14 (noting "valid, enforceable third-party contracts" Bright Data disrupted). The Copyright Act does not foreclose contract law from holding Bright Data to its bargain. Doing so neither frustrates the Copyright Act's fair-use policy nor impinges on Congress's conception of the public domain. *See Grosso v. Miramax Film Corp.*, 383 F.3d 965, 968 (9th Cir. 2004) (contract claims "turn[] not upon the existence of a [copyright]" but on contractual "promise") (cleaned up); *Davidson*, 422 F.3d at 639 (contractual fair-use waiver not preempted); *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 966-67, 977 (N.D. Cal. 2013)

[1] Most courts reject preemption of contract claims under the Copyright Act's preemption clause, without finding it necessary to address conflict preemption. *See, e.g.*, *Altera*, 424 F.3d at 1089. Of the "close to 300 court decisions on the preemption of contracts by the Copyright Act, fewer than ten even considered the question of implied preemption. Implied preemption, and in particular conflict preemption, have been addressed in only two federal appellate court decisions." Guy A. Rub, *A Less-Formalistic Copyright Preemption*, 24 J. Intell. Prop. L. 329, 347 (2017). Both of those decisions found no preemption. *See Ryan*, 786 F.3d at 761-62; *Davidson & Assocs. v. Jung*, 422 F.3d 630, 638 (8th Cir. 2005).

(breach-of-contract claims against scrapers not preempted despite "terms of use" granting Craigslist a "broad license to use and republish content submitted by its users.").

The Court held X's prior contract claims preempted based on fears that X seeks to "impose[]" a "massive regime of adhesive terms" that risks "alter[ing] the rights and privileges of the world at large." Op. at 20. The SAC clarifies that X's allegations do not go so far. The SAC (¶ 42) now disclaims any attempt to enforce X's users' copyrights, so X's claims cannot affect those users' ability to "exploit[]" their own "exclusive rights." Op. at 23. Indeed, if X prevails in this case, X's users will remain free to license their own posts directly to Bright Data, just as they will remain free to sue Bright Data for copyright infringement. SAC ¶ 42. X's contract claims usurp neither right. As the Terms make clear, the exclusive rights the Copyright Act vests in individual users for their own posts – reproduction and distribution, for instance – remain with X's users (subject to X's non-exclusive license). 17 U.S.C. § 106. So this Court can enforce X's own "contract agreements" with Bright Data without endorsing "the sort of state regulatory scheme that preemption primarily targets." *Craigslist*, 942 F. Supp. 2d at 977.

True, X's Terms are not bilaterally negotiated like a classic "contract between two sophisticated parties in which one or the other adjusts their rights." Op. at 20. But courts often reject copyright-preemption arguments involving similar unilateral contracts.[2] And Bright Data is a "sophisticated party" that had actual "knowledge of the Terms at all relevant times." *Id.* at 16-17; *see* SAC ¶¶ 96-104. The Court thus can leave for another day the hypothetical questions about a "regime of adhesive terms" that seeks to rewrite copyright entitlements for "millions of" unwitting users wanting to exploit their own posts. That is not this case. On these facts, enforcing the Terms *against Bright Data specifically* does not imperil any federal objectives.

[2] *See, e.g.*, *Altera*, 424 F.3d at 1089-90 (software licensing agreement not preempted); *MDY Indus., LLC v. Blizzard Ent., Inc.*, 629 F.3d 928, 957 (9th Cir. 2010) ("anti-bot provisions" of unilateral terms of use); *Bowers v. Baystate Techs., Inc.*, 320 F.3d 1317, 1323-26 (Fed. Cir. 2003) (shrinkwrap agreement); *Nat'l Car Rental Sys., Inc. v. Computer Assocs. Int'l, Inc.*, 991 F.2d 426, 432 (8th Cir. 1993) (software license); *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1453-55 (7th Cir. 1996) (shrinkwrap contract); *Craigslist*, 942 F. Supp. 2d at 977 (similar).

Non-contract claims. Nor does the Copyright Act preempt the SAC's remaining claims. The Court previously discerned three conflicts between the federal law and X's tort claims "based on scraping and selling of data." Op. at 23-25. The SAC resolves those conflicts, too.

To start, the SAC clarifies (¶ 39) that X's claims cover Bright Data's scraping of two distinct types of information on X's platform: (1) copyrightable content, like user-generated photos; and (2) non-copyrightable data, like follower lists, *see Feist*, 499 U.S. at 361-64 (arrangement of subscriber information in phone book not copyrightable). Bright Data scrapes both, and X asserts claims based on both. SAC ¶¶ 39-41. At a minimum, the latter cannot create conflict preemption. The Copyright Act, after all, disclaims preemption for works that do "not come within the subject matter of copyright." 17 U.S.C. § 301(b)(1). Such works cannot implicate Congress's lawful copyright objectives because "originality is a constitutionally mandated prerequisite for copyright protection." *Feist*, 499 U.S. at 351, 358-61.

X's claims therefore concern at least some information altogether outside the federal copyright regime, which defeats any copyright preemption. *See Dun & Bradstreet Software Servs., Inc. v. Grace Consulting, Inc.*, 307 F.3d 197, 218 (3d Cir. 2002) (no preemption because "customer lists are not subject to copyright"); *No Doubt v. Activision Publ'g, Inc.*, 702 F. Supp. 2d 1139, 1145-47 (C.D. Cal. 2010) (likeness was not copyrightable, so contract governing use of likeness as not preempted); *VocalSpace, LLC v. Lorenso*, 2010 WL 11527374, at *7 (E.D. Tex. Jan. 29, 2010) (no preemption for customer lists). Indeed, one Court in this District found no preemption of a similar claim alleging scraping of non-copyrighted emails from Facebook's platform. *See Facebook, Inc. v. ConnectU LLC*, 489 F. Supp. 2d 1087, 1092-93 (N.D. Cal. 2007). While Facebook's "site presumably include[d] [creative] works created by Facebook's users," the presence of *some* copyrightable works did not transform the "entire site" into a "work of authorship" subject to copyright preemption. *Id.* The same conclusion follows here.

The SAC's amended allegations (¶ 39) further disclaim the power to exercise "copyright owners' exclusive rights." Op. at 23. X's users retain all their copyrights in their individual posts, which they may assert (or not) against Bright Data as they wish. Meanwhile, X seeks to remedy something else: Bright Data's automated scraping of *aggregate* data from X's platform

at scale. SAC ¶¶ 39-41. X invested substantial money and ingenuity in developing a state-of-the-art platform that hosts and organizes that content, *id.* ¶¶ 80-81, and its massive scale – not any one post – is what scrapers covet, *id.* ¶ 41. X's interest in this aggregate data differs from its users' copyright interests in their own creative works. *See Compulife Software Inc. v. Newman*, 959 F.3d 1288, 1313-15 (11th Cir. 2020) (distinguishing between ordinary access to public data and "using a bot to collect an otherwise infeasible amount of data"); *hiQ*, 2021 WL 1531172, at *7 (recognizing platform's "'quasi-property' rights" against scraper even though platform "members, and not [the platform] itself, owns the information in their public profiles").

Nor do X's amended claims "interfer[e] with the exercise of the statutory privilege of fair use." Op. at 23. X's claims seek to remedy Bright Data's interference with X's state-law property right to the aggregate information organized on its platform. SAC ¶¶ 39-41, 182-86. Such claims do not foreclose Bright Data from invoking fair use as a defense to some future claim (which X has not brought) alleging copyright infringement of users' posts. *See Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 333, 343 (D. Mass. 2013) (fair use is a defense, not an affirmative right). In any event, Bright Data's scraping and reselling data is not fair use because it is not transformative; it is a non-original exploitation of X user data for commercial purposes. SAC ¶ 119; *see Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 537, 555 (S.D.N.Y. 2013) ("algorithm to crawl over and scrape content from the Internet" not fair use). X's amended claims thus do not "obliterate[]" federal fair-use protections, Op. at 24; such protections remain available to other defendants facing copyright claims on different facts.

Finally, the SAC clarifies that X's claims do not hinge on "content that X users designated for public use." *Id.* Even if individual user posts were "public" on their own, the aggregation of *all* those posts – which is what Bright Data wants – is not. SAC ¶¶ 39-41. Courts have recognized that key difference in upholding claims against other data scrapers. *See Compulife*, 959 F.3d at 1314 (using "robot" to "collect" more information than "any human practicably could" differs from using ordinary means to take data from "publicly accessible site"); *hiQ*, 2021 WL 1531172, at *7 (recognizing LinkedIn's "property rights" in aggregate collection of user profiles reflecting its own "labor, skill, and money") (cleaned up). Put simply,

this Court can stop Bright Data from vacuuming up all the data on X's platform without impeding others from exploiting public-domain works consistent with federal copyright law.

In any event, the SAC alleges much of the data on X that Bright Data and its customers are scraping is *not* available to the public. SAC ¶ 3. Instead, the data is available only to X users who are logged in and who agree to X's Terms. *Id.* ¶¶ 61-79, 122. So when users post content on X, they are not agreeing that Bright Data may scrape it with impunity. *Id.* ¶¶ 23-38. In fact, Bright Data scrapes user content without users' knowledge or consent. *Id.* ¶ 119. And it does so by creating fake accounts and circumventing safeguards X designed to limit the platform's content to authentic human users. *Id.* ¶¶ 3-4, 129-33. X has a legitimate state-law interest in stopping that behavior. *See eBay*, 100 F. Supp. 2d at 1070 (no preemption of trespass claim for "publicly accessible" data); *Digital Drilling Data Sys., L.L.C. v. Petrolink Servs., Inc.*, 965 F.3d 365, 380-81 (5th Cir. 2020) (data-scraping claim not preempted because "wrongful conduct" included "inducing" others to "violate the express terms of their . . . licenses").

b) X's claims promote substantial state-law interests independent of copyright

Even if there were a conflict, the Copyright Act does not preempt claims that "vindicate[] a substantial state law interest, i.e., an 'interest[] outside the sphere of congressional concern in the [copyright] laws.'" Op. at 25 (quoting *In re Jackson*, 972 F.3d 25, 37 (2d Cir. 2020)) (cleaned up). The SAC adds allegations identifying three such state interests.

i. Bright Data's Scraping Threatens X Users' Privacy

As this Court observed, the Copyright Act does not preempt state privacy laws because "the protection of privacy is not a function of the copyright law." Op. at 25 (quoting *Garcia v. Google, Inc.*, 786 F.3d 733, 745 (9th Cir. 2015)). The Supreme Court held decades ago that the Patent Act does not preempt state-law trade-secret-misappropriation claims because states retain a sovereign interest in protecting that "most fundamental human right, that of privacy." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 487 (1974). The same is true here.

X's state-law claims promote substantial state-law interests in user privacy. To gain access to much of X's content and data, users must register accounts and agree to X's Terms of Service, Privacy Policy, and other Rules and Policies. SAC ¶¶ 23-38, 61-79. The Privacy Policy

allows X users to adjust their privacy settings, opt out of data sharing, and select which of their content is made public. *Id.* ¶ 36. Users may also delete their content at any time, including by making deletion requests under the California Consumer Privacy Act ("CCPA") or the European Union's General Data Protection Regulation. *Id.* ¶¶ 36-38. To facilitate those protections, X implements myriad restrictions blocking non-registered users and bots from accessing user data. *Id.* ¶¶ 58-79. X designed all these measures to safeguard its users' privacy. *Id.* ¶¶ 93-95, 135.

Bright Data runs roughshod over those protections. Unlike X, Bright Data places virtually no restrictions on the use of the data it collects. *Id.* ¶ 136. It does not, for example, deny (or stop its customers from) taking steps to identify users based on protected characteristics, or from tracking their location. *Id.* ¶¶ 4, 136(b)-(e). To the contrary, Bright Data's website hawks mass-collected "location" information of X's users. *Id.* ¶ 124. Bright Data likewise does not require the deletion of data associated with users who adjust their privacy settings or who delete their accounts. *Id.* ¶¶ 135, 136(a). So unlike on X's platform, once Bright Data scrapes and sells a user's data, that user has no realistic way to retrieve it. *Id.* ¶¶ 51, 136. Given that Bright Data appears to sell user data to anyone and everyone – including governments and malign actors – the privacy concerns that result are acute. *Id.* ¶¶ 49, 136(e).

X's own developer program is different. The Court read X's last complaint to allege no legitimate interest in "X users' privacy" because X "allow[s] the extraction of copying of X users' content so long as it gets paid." Op. at 25. The SAC clarifies that X's sale of user data bears no resemblance to what Bright Data does. Unlike Bright Data, X imposes strict privacy measures on developers who access data through X's API services. SAC ¶¶ 48-51. All developers are bound by X's Developer Agreement, which requires (among other things) user consent before developers may use their content for promotions. *Id.* Developers also may not use user data to infer protected characteristics like financial status or health; may not match X data with other identifiers without the user's express consent; and may not track or target sensitive groups, including based on location. *Id.* ¶ 51 (f)-(j). And if a user modifies or deletes his own content, X and its developers must do the same. *Id.* ¶¶ 48-51.

X takes those steps to attract users and to safeguard their privacy interests. *Id.* ¶¶ 22, 52-57. Bright Data's unauthorized scraping undermines both goals. As an intergovernmental body recently highlighted in a "Joint statement on data scraping and the protection of privacy," scraping from social-media platforms like X poses grave threats to user privacy.[3] Those threats to users include targeted cyberattacks, identity theft, profiling, foreign surveillance, and spam. *Id.* The report thus encouraged platforms to guard against scraping by deploying rate limits, bot detection, CAPTCHA, and IP blocking. *Id.* X employs those very measures to combat scraping and protect its users' privacy. *Id.* ¶¶ 60-79. Yet Bright Data circumvents X's safeguards and encourages its customers to do the same. *Id.* ¶¶ 79, 104-34.

California and X retain a strong, non-copyright interest in guarding against such privacy intrusions. *See Stackla, Inc. v. Facebook Inc.*, 2019 WL 4738288, at *6 (N.D. Cal. Sept. 27, 2019) ("Facebook's ability to decisively police the integrity of its platforms is without question a pressing public interest" including "protection of its users' privacy."); *ACLU v. Clearview AI, Inc.*, 2021 Ill. Cir. LEXIS 292, at *22-23 (Ill. Cir. Ct. Cook Cnty. Aug. 27, 2021) (rejecting argument that users had "no expectation of privacy" in "publicly-available" photographs in privacy suits against scraper). Even for publicly available data, X's users retain privacy interests that Bright Data is usurping. For example, California law protects consumer privacy even for data publicly shared online, which X zealously enforces. *See* Cal. Civ. Code § 1798.100 *et seq.* Whenever users post content on X, even publicly, they do so in reliance on X's Terms and its privacy protections, scraping restrictions, and compliance with laws like the CCPA. SAC ¶¶ 36-38, 51(h), 52-57, 95. X's claims vindicate those non-copyright interests.

ii. Bright Data's Scraping Enables Data Misuse By Malign Actors

X's state-law claims also promote non-copyright interests in data security. When X allows developers to access user data through its API tiers, it takes steps to ensure that malign actors cannot misuse the data. SAC ¶¶ 49-51. IP addresses from "high-risk jurisdictions," for

[3] Info. Comm'rs Off., *Int'l Enf't Coop. Working Grp., Joint Statement on Data Scraping and the Protection of Privacy* (Aug. 24, 2023), https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf.

example, are "blacklist[ed]" from accessing X data altogether. *Id.* ¶ 49. Consistent with those efforts, X has removed thousands of accounts linked to hostile countries like Iran. *Id.* ¶ 55. Similarly, X bars governments from using the API to collect user data, because of the surveillance risks. *Id.* ¶ 49. And X requires subscribers to its highest-volume API tier to submit their proposed "use cases" for X to screen before they may tap into any user data. *Id.* ¶ 48. X has refused access to prospective developers because of their links to malign actors or related concerns about their proposed use cases. *Id.*

Bright Data's conduct vitiates those protections. It appears willing to sell scraped data to anyone, anywhere, for any purpose. *Id.* ¶ 136. It also sells scraping tools to its own customers, compounding the risks that those customers will in turn supply X's data to malign actors. *Id.* ¶¶ 121-34. And it does all this while promising its customers "total anonymity." *Id.* ¶ 131. The potential security risks this creates are legion. Once Bright Data vacuums up X's data and releases it outside the controlled environment of X's APIs, X loses the ability to control or even track downstream uses of that data. *Id.* ¶ 135. Nothing stops Bright Data or its customers from secretly taking X's scraped data and selling it to terrorists or other bad actors.[4]

X has a non-copyright state-law interest in stopping such conduct. States have long encouraged private companies to maintain secure networks because of the harm data breaches cause for the companies, their platforms, their customers, and even states themselves.[5] California (like other states) has enacted data breach notification law, to incentivize companies to guard against user data falling into the wrong hands. *See, e.g.*, Cal. Civ. Code § 1798.82. And several states have enacted stringent cybersecurity laws, setting standards for private business and punishing those who enable unauthorized access to user data.[6] X's state-law claims

[4] *Cf.* Exec. Order No. 14,117, 89 Fed. Reg. 15421 (Mar. 1, 2024) (barring sale of commercially available personal data to entities in adversarial countries due to potential misuse).

[5] *See* Michael Glennon, *State-Level Cybersecurity*, Hoover Inst. Pol'y Rev. (Feb. 1, 2012), https://www.hoover.org/research/state-level-cybersecurity (for cyber security, "the dangers posed clearly implicate the police powers traditionally exercised by the states"); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154 (D. Minn. 2014) (state-law claims for data breach).

[6] *See, e.g.*, Cal. Penal Code § 502 (preventing unauthorized access); N.Y. Codes R. & Regs. tit. 23, § 500 (requiring business to develop and maintain cybersecurity programs).

vindicate these interests. *See Anthem*, 162 F. Supp. 3d at 990 (recognizing "California's public policy of protecting customer data") (cleaned up). The federal interests that the Copyright Act protects are different and so do not preempt such claims. *See Craigslist, Inc. v. Autoposterpro, Inc.*, 2009 WL 890896, at *3 (N.D. Cal. Mar. 31, 2009) (no preemption of Cal. Penal Code § 502 because restrictions on unauthorized access are distinct from copyright).

iii. Bright Data's Scraping Undermines Consumer-Protection Interests

X's state-law claims further advance consumer-protection interests. Courts often reject federal preemption of claims that promote consumer protection, including in actions instituted by private parties like X. *See, e.g., In re JUUL Labs, Inc., Mktg., Sales Pracs., & Prods. Liab. Litig.*, 497 F. Supp. 3d 552, 584, 592-93, 666 (N.D. Cal. 2020) (declining to hold that the FDA's regulations preclude product liability claims or consumer protection laws); *Jackson*, 972 F.3d at 35, 37-38 ("preventing consumer deception" is substantial state interest). The Second Circuit, for example, held that a federal consent decree did not impliedly preempt a state consumer law "[b]ecause consumer protection law is a field traditionally regulated by the states." *General Motors Corp. v. Abrams*, 897 F.2d 34, 41-42 (2d Cir. 1990).

X designed its developer policies in part to protect its users from manipulation. SAC ¶¶ 39-57. Those policies reflect X's concern that scraped data can be used to target and defraud users through misleading advertisements, spam, or phishing. *Id.* Indeed, X maintains strict control over third-party access to X user data in part to limit this kind of consumer harm. *Id.* That is another reason why X requires developers who want access to X's data to submit their proposed use case, agree to additional terms, delete or modify data as requested, and avoid using X's data to unmask or target users. *Id.* ¶¶ 48-51. X can also better track and respond to data misuse by those who pay for a subscription versus the anonymous scraping Bright Data enables. *Id.* ¶ 57. Allowing just anyone to anonymously access X user data at scale, which is what Bright Data does, undermines X's ability to police its platform against such manipulation. *Id.* ¶ 135.

B. The SAC Sufficiently Pleads Three Additional Claims

The SAC also adds claims for violations of the Digital Millennium Copyright Act, the Computer Fraud and Abuse Act, and California's Comprehensive Computer Data and Access

Fraud Act. Courts in this Circuit often grant leave to file amended complaints with new claims. *See, e.g., Wang v. Zymergen Inc.*, 2024 WL 773603, at *3 (N.D. Cal. Feb. 26, 2024) (finding no prejudice from new claim because "granting leave to amend is not dependent on whether the amendment will add causes of action or parties." *DCD*, 833 F.2d at 186; *Fishman v. Tiger Nat. Gas, Inc.*, 2018 WL 2552597, at *2 (N.D. Cal. June 4, 2018) (Alsup, J.) (granting leave to "add new claims"). And because the SAC sufficiently pleads those claims, leave is not futile.

1. The Digital Millennium Copyright Act ("DMCA")

The Court should permit X to add a DMCA claim. SAC ¶¶ 189-99. The DMCA prohibits "circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act]." 17 U.S.C. § 1201(a)(1)(A). A related provision bars "(1) traffic[king] in (2) a technology or part thereof (3) that is primarily designed, produced, or marketed for, or has limited commercially significant use other than (4) circumventing a technological measure (5) that effectively controls access (6) to a copyrighted work." *MDY*, 629 F.3d at 953 (citing 17 U.S.C. § 1201(a)(2)). Bright Data violated both provisions.

X owns copyrights in its websites and mobile app. SAC ¶ 190.[7] It also deploys an array of technological measures to effectively control access to and prevent automated systems from accessing those websites and app – including CAPTCHAs, robots.txt files, registered user identification limits, IP rate limits, and anomaly-detection tools. *Id.* ¶¶ 64-82; *see Ticketmaster L.L.C. v. Prestige Ent. W., Inc.*, 315 F. Supp. 3d 1147, 1166-67 (C.D. Cal. 2018) (sustaining DMCA claim against data scraper for using bots to circumvent "security measures, including CAPTCHA" that "control access to Ticketmaster's copyrighted webpages"). As noted, most of X's valuable data is locked behind these technological measures. SAC ¶¶ 3, 25-28, 64-79. Bright Data's use of automated systems to engage in widespread scraping of data from X's platform circumvents these measures in violation of § 1201(a)(1)(A). *Id.* ¶¶ 79, 105-32. And as its website makes clear, Bright Data sells proxy services and other tools that are "primarily

[7] Those copyrights differ from the copyrights held in the underlying creative works reflected in individual user posts, which remain with X's users. SAC ¶ 42. X's DMCA claim does not hinge on access to user content, but on access to the copyrighted website and app that host the content.

designed, produced, or marketed for," and have no "commercially significant use other than," *MDY*, 629 F.3d at 953, circumventing X's anti-scraping measures, SAC ¶¶ 121-34. These facts are sufficient to plead a violation of § 1201(a)(2). *See MDY*, 629 F.3d at 953.

2. The Computer Fraud and Abuse Act ("CFAA")

The Court should also permit X to plead a CFAA claim. SAC ¶¶ 200-11. The CFAA prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). This prohibition applies "to all information from all computers that connect to the Internet," *Van Buren v. United States*, 593 U.S. 374, 379 (2021), including X's servers. "[W]ithout authorization" is "a non-technical term that . . . means accessing a protected computer without permission." *United States v. Nosal*, 844 F.3d 1024, 1028 (9th Cir. 2016). A scraper accesses a computer system "without authorization" when it "circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access." *hiQ*, 31 F.4th at 1201; *see Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1261, 1277 (N.D. Cal. 2022) (using fake accounts to collect password-protected non-public pages violated CFAA).

Bright Data has done just that. X alleges that Bright Data has circumvented its technological barriers and access restrictions to engage in widespread scraping of data that is accessible only to those who are logged into registered, password-protected accounts. SAC ¶¶ 25-28, 64-82, 105-34. For instance, Bright Data scrapes massive volumes of data accessible only to logged-in users by bypassing IP rate limits that would otherwise prevent scraping by redirecting users to the log-in page. *Id.* Moreover, the volume of data Bright Data scrapes can be achieved only through the creation of fake X accounts and automated systems bypassing X's CAPTCHA prompts and other access restrictions. *Id.* Courts have found similar allegations sufficient to plead a CFAA claim. *See BrandTotal*, 605 F. Supp. 3d at 1261 (noting that "Meta allows non-authenticated users to access certain ad URLs a very limited number of times, it then redirects them to a log-in page and prevents further access") (cleaned up); *Ryanair DAC v. Booking Holdings Inc.*, 636 F. Supp. 3d 490, 509 (D. Del. 2022) (airline stated claims against

travel booking companies and their aggregators for violation of CFAA by screen scraping data where airline alleged users were required to log into website using a username and password).

Bright Data has also induced others to intentionally access X's servers without authorization by selling and advertising tools designed to circumvent X's anti-scraping measures. SAC ¶¶ 105, 121-134. Bright Data is thus vicariously liable for those users' violations of the CFAA as well. *See Facebook, Inc. v. Power Ventures, Inc*., 844 F.3d 1058, 1066-67 (9th Cir. 2016) (acknowledging potential for vicarious liability under § 1030(g)); *Ryanair*, 636 F. Supp. 3d at 499 ("[V]icarious or indirect liability . . . extends to parties who direct, encourage, or induce others to commit acts that violate the [CFAA]."); *Synthes, Inc. v. Emerge Med., Inc*., 2012 WL 4205476, at *17 (E.D. Pa. Sept. 19, 2012) ("[M]any courts have found that one's act of inducing another to access a computer that he or she is otherwise not authorized to use constitutes 'access' for purposes of CFAA liability.").

Further, the CFAA prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value." 18 U.S.C. § 1030(a)(4). Bright Data's proxy services conceal the true requestor's IP address and location, allowing unregistered users to impersonate registered X users. SAC ¶¶ 108-13, 123-34; *see Ryanair*, 636 F. Supp. 3d at 507 (upholding allegations that defendants and data aggregators "engaged in fraudulent conduct by misrepresenting themselves, for example by 'lying about [their] email address[es] or anonymizing [their] IP address[es],' when creating accounts") (cleaned up). Bright Data's tools also allow its customers to access X via proxy servers even when X has previously blocked their IP addresses – that is why Bright Data tells customers they can scrape without being "flagged or blocked" by IP-blocking measures. SAC ¶¶ 1, 132.

Bright Data's conduct has caused X substantial losses, including those associated with the increased burden on X's website and the engineering efforts necessary to remediate Bright Data's unauthorized scraping. *Id.* ¶¶ 89-95. Those losses far exceed the CFAA's $5,000 threshold. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I); *id.* § 1030(e)(11) (defining "loss" broadly). X's allegations therefore state a claim for multiple violations of the CFAA.

3. California's Computer Data Access and Fraud Act ("CDAFA")

Bright Data's alleged conduct also violates the CDAFA. SAC ¶¶ 212-17. That statute imposes liability on, among other things, any person who (a) "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network"; (b) "[k]nowingly and without permission uses or causes to be used computer services"; (c) "[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section"; or (d) "[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network." Cal. Penal Code § 502(c)(2)-(3), (6)-(7).

The CDAFA is even broader than its federal counterpart. Unlike the CFAA, the CDAFA "does not require unauthorized access. It merely requires knowing access." *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015); *see also NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 950 (N.D. Cal. 2014) (parties act "without permission" for purposes of statute when they circumvent technical or code-based barriers limiting user access); *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1057 (N.D. Cal. 2010) (website operator stated claim against software developer where developer knowingly accessed its computer system and provided means for others to do so in violation of Terms of Use). Bright Data not only circumvented several technical measures designed to prevent scraping data on X's platform (and caused others to do the same), but it did so knowingly in violation of the Terms. SAC ¶¶ 29-35, 79, 96-134. That conduct violates multiple CDAFA provisions for the reasons stated above.

C. X's Amendments Are Timely And Do Not Prejudice Bright Data

Rule 15(a)(2) furnishes no other grounds on which to deny X's Motion. There has been no "undue delay." *Shelton*, 2024 WL 234721, at *1. The Court invited X to propose an amended complaint by June 6, Op. at 26, which X timely did, Dkt. 90. At that point, the case was not even a year old. Dkt. 1. After the Court disqualified X's prior counsel, it invited new counsel "to move for leave to amend its complaint" by August 16. Dkt. 105 at 15. X now files this Motion under the Court's order. Courts in this Circuit often allow similar amendments more than a year into the case. *See, e.g., DCD*, 833 F.2d at 185, 187 (14 months). Delays aside,

absent "undue prejudice" courts "should ordinarily permit a party to amend." *Howey v. United States*, 481 F.2d 1187, 1190 (9th Cir. 1973) (reversing denial of leave after five-year delay).

Bright Data cannot carry its "burden of showing prejudice." *DCD*, 833 F.2d at 187. To "overcome Rule 15(a)'s liberal policy with respect to the amendment of pleadings[,] a showing of prejudice must be substantial." *MagTarget LLC v. Saldana*, 2019 WL 1904205, at *3 (N.D. Cal. Apr. 29, 2019) (cleaned up). No such prejudice exists here. Prejudice typically requires a showing that the deadline for amendments has passed or that discovery is nearing completion. *See Dep't of Fair Emp. & Hous. v. L. Sch. Admission Council, Inc.*, 2013 WL 485830, at *5-6 (N.D. Cal. Feb. 6, 2013) (collecting cases). Neither is true here, where X complied with the Court's deadline and where discovery remains in its infancy.

The SAC's three new claims do not change the calculus. *See Nelson v. Matrixx Initiatives, Inc.*, 2012 WL 1094316, at *2 (N.D. Cal. Mar. 30, 2012) (Alsup, J.) (no prejudice from new claims). The "liberality in granting leave to amend is not dependent on whether the amendment will add causes of action." *DCD*, 833 F.2d at 186. "[A]dding new claims" may require Bright Data "to defend against those claims," but that "does not constitute undue prejudice." *Wang*, 2024 WL 773603, at *3. This is especially true because X's new claims are based on similar facts as the existing claims, which gave Bright Data "notice that these claims existed." *Johnson v. Serenity Transp., Inc.*, 2015 WL 4913266, at *5 (N.D. Cal. Aug. 17, 2015).

The remaining Rule 15(a)(2) factors are similar. X has not acted in "bad faith." *See Grinder v. Experian Info. Sols., Inc.*, 2017 WL 3478845, at *2 (N.D. Cal. Aug. 14, 2017) (Alsup, J.). Nor has X repeatedly failed to cure any deficiencies; the Court has not yet reached the merits of any other motion for leave to amend. Given the "extreme liberality" with which courts allow amendment, *Eminence*, 316 F.3d at 1051 (cleaned up), the Court should thus accept the SAC.

V. CONCLUSION

For the foregoing reasons, X Corp. respectfully requests that the Court grant X's Motion for Leave To File a Second Amended Complaint.

DATED: August 16, 2024

Respectfully submitted,

KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.

By: /s/ Joshua D. Branson

JOSHUA D. BRANSON*
jbranson@kellogghansen.com
DANIEL V. DORRIS*
ddorris@kellogghansen.com
BETHAN R. JONES*
bjones@kellogghansen.com
MATTHEW D. READE*
mreade@kellogghansen.com
TIBERIUS T. DAVIS*
tdavis@kellogghansen.com
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
Telephone: 202.326.7900
* *Admitted Pro Hac Vice*

Adrian Sawyer, State Bar No. 203712
SAWYER & LABAR LLP
1700 Montgomery Street, Suite 108
San Francisco, California 94111
Telephone: 415.262.3820
sawyer@sawyerlabar.com

Attorneys for Plaintiff X Corp.